UNITED STATES PATENT AND TRADEMARK OFFICE

H·D

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/763,275	01/26/2004	Kousetsu Sai	1466.1084	6491

21171 7590 04/12/2007
STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
BAYOU, YONAS A	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/763,275	**Applicant(s)** SAI, KOUSETSU	
	Examiner Yonas Bayou	**Art Unit** 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/26/04*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 8 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 8 is directed initiating performance of transmitting rule information, receiving process information, monitoring the encryption of information and warning the information management system.

This claimed subject matter lacks a practical application of a judicial exception (law of nature, abstract idea, natural occurring phenomenon) since it fails to produce a useful, concrete and tangible result.

Specifically, the claimed subject matter doesn't produce tangible result because the claimed subject matter fails to produce a result that is limited to having real world value rather than a result that may be interpreted to be abstract in nature as, for example a computer program. More specifically, the claimed subject matter provides a computer program product for use in a computer supporting encryption of information for an information management system that manages information. This produced result remains in the abstract and, thus, fails to achieve the required status of having real world value.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 3 and 5-8 are rejected under 35 U.S.C. 102(b) as being anticipated by Choo Patent No. US 6,981,140.

Referring to claims 1, 5, 6 and 8 Choo teaches a security system comprising an information management system (equivalent to "second memory area/user space/user memory", 201 in fig. 2 and column 1, lines 39-49) for managing information and an encryption support system (equivalent to "first memory area/Kernel space or Kernel/operating system (OS)") for supporting encryption of information in the information management system, the encryption support system including:

an encryption rule storing portion for storing rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret **[column 11, lines 3-6**; security policy database 602 in fig. 6, inherently stores an encryption rule],

an encryption data transmitting portion for transmitting encryption data that is necessary for encrypting information in accordance with the rule to the information management system **[column 6, lines 18-19; column 10, line 65 - column 11, line 3; fig. 6**; transmit data after "checked by the internet protocol security stack 510 against a security policy database 602" which is equivalent to rule information],

a process information receiving portion for receiving process information that indicates the encryption process performed by the information management system from the information management system **[column 6, lines 20-25,** the encryption data is processed in second memory area which is inherently in the information management system; wherein the first memory area is equivalent to the encryption support system is receiving processed information],

a monitoring portion for monitoring whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system, and **[column 10, line 65 - column 11, line 3; column 13, lines 14-20 and fig. 10;** the internet protocol security stack 510 in fig. 6 is inherently the monitoring portion for monitoring whether the encrypted data received is processed according to the rule/policy prior to transmission].

a warning portion for warning the information management system that was found to encrypt information not in accordance with the rule by the monitoring portion to do encryption of information in accordance with the rule, and **[column 11, lines 6-19 and fig. 6**; the internet protocol security stack 510 in fig. 6 (equivalent to a warning portion as well) detects and warns "an Internet Key Exchange (IKE) block 604, in fig. 6" which resides in the user memory (i.e., information management system) that the encrypted information found is not in accordance with the rule].

Choo also teaches the information management system (equivalent to "second memory area/user space/user memory", 201 in fig. 2 and column 1, lines 39-49) including:

an encryption data receiving portion for receiving the encryption data from the encryption support system **[column 6, lines 3-5],**

a classification secret level storing portion for storing classification of information managed by the information management system in connection with the secret level for each of the classification **[column 11, lines 3-6**; a classification secret level is equivalent to a data packet (i.e., an encryption data) strored in a security policy database 602 which describing a security policy inherently the secret level for the classification] and

an encrypting portion for encrypting information managed by the information management system by using the encryption data of the secret level corresponding to the classification of the information received by the encryption data receiving portion **[column 6, lines 20-25]**,

an information storing portion for storing the information encrypted by the encrypting portion, and a process information transmitting portion for transmitting the process information about the encryption performed by the encrypting portion to the encryption support system **[column 10, line 63-column 11, line 19;** teaches everything the same as the encryption support system (see above) which is vice versa, "the data is packetized and redirected via the redirector layer within the network protocol stack to the software port 509"].

Referring to claim 3, Choo further teaches, wherein the information management system includes:

a classification secret level transmitting portion for transmitting classification secret level information that indicates classification of information managed by the information management system and the secret level corresponding to the classification to the encryption support system **[column 6, lines 18-19; column 10, line 65 - column 11, line 3 and fig. 6,** a classification secret level is equivalent to a data packet, which is inherently an encryption data], and

the monitoring portion performs the monitoring by comparing the process information received from the information management system with the classification secret level information **[column 10, line 65 - column 11, line 3].**

Referring to claim 7, Choo teaches a security system, further comprising a validity monitoring portion (internet protocol security stack 510) for monitoring validity of an encryption rule that is used currently in accordance with vulnerability information about vulnerability of security received from a security information providing portion **[column 10, line 65 - column 11,**

line 19; for transferring information, it should be checked by the internet protocol security stack 510 validates and checks the security policy of the information to be transmitted/received], wherein

the transmitting portion transmits the encryption data for changing the rule appropriately to the information management system if it is decided that the encryption rule that is used currently has little validity **[column 6, lines 18-19; column 10, line 65 - column 11, line 13; fig. 6.**; for transmitting the encryption data if the data has not received a security association/security, an Internet Key Exchange(IKE) block 604 initiate a negotiation procedure with a corresponding respective internet keying agent which inherently changing the rule appropriately if the encryption rule that is used currently has little validity].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Choo US Patent No. US 6,981,140 in view of Iitsuka et al. US Patent No. 6,463,151.

Referring to claim 2, Choo teaches a security system comprising an information management system for managing information. Choo further teaches an encryption support system for supporting encryption of information in the information management system [see claim 1 above]. Choo does not explicitly teach a security system, wherein the rule information indicates the rule including an encryption system that is used for encryption and a valid term of an encryption key that is used for the encryption. However, Iitsuka teaches a security system, wherein the rule information indicates the rule including an encryption system that is used for encryption and a valid term of an encryption key that is used for the encryption,

if a period since the information management system encrypted information until the present time exceeds the valid term relevant to the rule of the secret level corresponding to the classification of the information **[column 3, lines 56-62 and fig. 4,** update the type of encryption by time scale according to a change over information/data i.e., copy one generation, copy freely and copy-prohibited (column 4, lines 45-50)],

the warning portion warns the information management system **[column 9, lines 18-35; column 12, line 63-column 13, line 8 and figs. 2 and 4;** in-transition mode (01 is assigned in fig. 4) is equivalent to the warning portion warns/notifying the timing for changing over the key or encryption which inherently teaches a period or time should not be exceeds the valid term relevant to the rule of the secret level],

if the encryption system that is indicated in the rule information is changed,

the encryption data transmitting portion transmits the encryption data for performing encryption with the changed encryption system to the information management system **[column 4, lines 33-39;** after update the type of encryption by time scale according to a change over information/data, transmission of encryption data will take place],

the warning portion warns to perform encryption of information in accordance with the changed encryption system **[column 9, lines 18-35; column 12, line 63-column 13, line 8 and figs. 2 and 4;** in-transition mode (01 is assigned in fig. 4) is equivalent to the warning portion warns/notifying the timing for changing over the key or encryption which inherently teaches a period or time should not be exceeds the valid term relevant to the rule of the secret level].

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Choo to incorporate a valid term of an encryption key that is used for the encryption of Iitsuka because determining a key which is used for the encryption applied to transmitted data is changed depending on the content of copy management information for the data. Thus, the transmitted data can be further securely protected.

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Choo US Patent No. US 6,981,140 in view of Albrecht et al US Patent No. 6,510,521.

Referring to claim 4, Choo teaches a security system comprising an information management system for managing information. Choo further teaches an encryption support system for supporting encryption of information in the information management system [see claim 1 above]. Choo does not explicitly teach the security system comprising a valid term managing portion for managing a valid term of a certification for affixing an electronic signature to information. However, Albrecht teaches a security system comprising a valid term managing portion for managing a valid term of a certification for affixing an electronic signature to information, wherein

the monitoring portion monitors whether or not it is necessary to reaffix the electronic signature to the information in accordance with the valid term of the certification, and **[column 1, lines 35-41**; "generates electronic signature and attached to a transferable unit of data" inherently teaches monitoring the information by reaffixing the electronic signature to the information in accordance with the valid term of the certification].

the warning portion warns the information management system for managing the information to reaffix the electronic signature if it is decided that it is necessary to reaffix the electronic signature **[column 2, lines 57-62;** the electronic signature is attached at the time write data (system basic input/output service (BIOS) update, such as additions, deletions and modifications) is created, inherently teaches reaffix the electronic signature to information].

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Choo to incorporate a valid term of a certification for affixing an electronic signature to information of Albrecht because generating and attaching electronic signature to a transferable unit prevents unauthorized write access to a protected storage such as FLASH mamory.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

YB

Kim Nguyen

Kimberly D. Nguyen
Primary ExamineR